# INTERNET OF THINGS – BLUETOOTH

The advancements in technology have brought about vast improvements and ease to our daily lives. The Internet has played a huge role in achieving this. Evolution of mobile, home, and embedded applications being connected to the internet, more commonly known as the internet of things (IoT) has integrated greater compute capabilities using data analytics to extract meaningful information. Billions of devices and their related devices connect to form an intelligent system of systems and share data across the cloud to analyze it and has provided us with ways to work faster, more efficiently, and with lower development costs. Practically all appliances can now be connected to the internet. For example, a smart home. Home appliances like doors, ACs, smoke detectors and security can be interconnected to share data with the user over a simple mobile application. In this essay I will be looking into one of the key networking wireless technologies that is widely used, which is Bluetooth.

Bluetooth is used in Wireless Personal Area Networks (WPAN) and can communicate approximately up to 10m. It is mostly used in local areas and for personal devices such as headsets, smartphones, and speakers. It is used in low power consumption and is cheaper than Wi-Fi. It uses 2.4 to 2.485 GHz ISM band. It is specified by an industry consortium called the Bluetooth Special Interest Group. It specifies an entire suite of protocols, going beyond the link layer to define application protocols, which it calls profiles, for a range of application. There’s a separate profile for each application. A piconet contains one master node and up to 7 slave nodes. Meaning, Bluetooth can connect to 8 devices at the same time without any interference from other wireless items, unlike Wi-Fi which interrupts connection among devices. Any communication is between the master and a slave, the slaves do not communicate directly with each other. Slaves can be parked or set to an inactive, low power state when not in use. A collection of piconets is called a scatternet. Like every other thing, Bluetooth has its pros and cons too. It can connect fixed and mobile devices. It is very low cost and easy to use and connect without the hassle of wires. However, it is slow compared to other technologies and only offers a small range and can be less secure. Even though this is the case, through our developing technology Bluetooth has become more secure than what it had been before and can be improved more in a near future.

Bluetooth can be classified into two types, which is Classic Bluetooth and Bluetooth Low Energy (BLE). BLE is used in devices that are powered by batteries and in sensors. It plays the role of the critical communication layer in IoT architecture. It bridges the hardware, software, and application layer together through multi-layer stack, including data link, network or transport and session protocols. Bluetooth connects sensor to sensor or sensor to gateway and is part of the data link layer. The routing or moving of packets across the network is the responsibility of the network layer which strategically uses the most appropriate paths to do so. Messaging is enabled across various elements of the IoT communication subsystem through the session layer protocols. Bluetooth has enabled IoT connectivity to be stepped up to the next level and is being increasingly used across industries. These industries include healthcare, automotive homes, entertainment and even security. It has allowed the reduction of manual tasks and has enhanced operational efficiency. This makes Bluetooth-powered IoT a big differentiator for most companies. BLE is also great for use in home environments. Most smart home devices use Bluetooth due to the convenience of the devices being at a proximity to each other and can create a mesh network that is self-healing. Meaning, if one device disconnects, all others can still stay connected and communicate with one another. These helpful features make Bluetooth an asset for the Internet of Things.

Some other wireless technologies used in IoT include Wi-Fi and LoRaWAN. These wireless network systems are easy to setup, cheaper to install and maintain. Bluetooth tends to be less battery hungry than Wi-Fi but can be more power-hungry than LoRa unless you are using low energy Bluetooth. However, it still covers a shorter range than LoRa making it more suitable for devices within a closer range. Wi-Fi on the other hand is superior when it comes to bandwidth but suffers when it comes to battery life and range. Bluetooth Low Energy uses the Lowest Power among these three protocols. Longest range goes to LoRa, No single technology can address all the IoT requirements. However, all of them are driving forces to the advancements in IoT. Learning how these forces can work along with each other can help build up on each of its strengths.

Although with the advancements and improvement of these technologies for IoT, risk factors remain and should be kept in mind. The Internet of Things is spreading further, more devices are connected to the Internet which makes things easier but also makes us more vulnerable and opens doors for hacking. Third party cloud storage systems can jeopardize our privacy and could also enable sensitive data leaks to the wrong hands. Protocol related attacks could occur among Bluetooth devices as well. For the most part, Bluetooth has been fairly secure. However, there have been a few instances where this security has been breached. Two instances associated with the insecurity of Bluetooth are Bluejacking and Bluesnarfing. Bluejacking is the sending of an unsolicited message to another device via Bluetooth. However, the Bluetooth standard has been updated and Bluejacking is not something that can occur anymore. A more significant Bluetooth vulnerability was Bluesnarfing, which is access to a Bluetooth-enabled device and transfer data. Fortunately, with the recent updates, Bluetooth has quickly patched this issue too and we haven’t seen this type of security vulnerability with Bluetooth again but it’s something we’re always looking for to make sure that our wireless networks are as secure as possible.

IoTs are very useful, however many of the devices have poor security and it can be very easy for ethical hackers to gain access to personal information and access other networks its connected to. IoT devices are being used in a distributed denial of service attack. Essentially, an IoT device is a small computer connected to the internet and can be infected with malware like any other device. This can create a botnet, meaning a network of malware infected devices which can control these devices remotely without the owner knowing. This could even lead to overloading of servers by sending so many messages, more than it could cope and it stops functioning properly. These attacks happen regularly. The motives of these happening range from hackers testing their skills, to activists making political or social points, criminals extorting money and sponsored agents attacking large scale infrastructures. If a device can communicate with another device, there’s always the potential of being hacked into the network that the device is connected to. To avoid this happening, there are ways to make the Internet of Things more secure. A network is only as secure as its weakest point of entry. Therefore, we should keep track of all the IoT devices we own and beware of older version of products which tend to have little security. Default passwords should be replaced with stronger unique ones. Device firmware should always be kept up to date. Product manufacturer reputation for internet security must be checked before the purchase of any device. The internet of things brings many advantages and is growing rapidly and is being used to create smart cities, businesses, and homes. Being aware of the way these devices are being exploited and taking these simple precautions will help keep your devices, homes, and families well protected.

Internet Of Things have had a huge impact on our lives. It has made our day-to-day activities easier and more flexible while also introducing us to several other protocols if one is not suitable. Although we rely on these now every day, there should be security precautions and measures taken regularly and beforehand to keep our personal information safe and secure. IoT is still evolving and reinventing ways for the future. The continued growth of IoT can be a transformative force for the future, if handled well and within the right hands.

## REFERENCE